

## CSB acorda prioritate IT Governance

---

Toate procesele vitale pentru activitatile unei companii moderne sunt sustinute de infrastructura IT (Information Technology – tehnologia informatiei). Astfel, sistemele informatice – adica echipamente, aplicatii, date, comunicatii si relatiile dintre acestea - au devenit extrem de importante, si in unele cazuri indispensabile, in sustinerea activitatii acestor companii. Dependenta critica a unei afaceri de sistemele informatice nu trebuie insa asociata cu o conotatie negativa. Dimpotriva, sustinerea asigurata de tehnologiile informatice proceselor de initiere, inregistrare, mutare, gestionare a tranzactiilor economice, informatiilor si cunostintelor, face ca acestea sa fie mai flexibile si mai eficiente. Totusi, rolul critic pe care sistemele informatice il au in managementul unei organizatii transforma disponibilitatea si conformitatea de functionarea acestora intr-un element esential. Mai mult, derapajele conjuncturale, dar si intreruperile planificate pentru mentenenta, conduc la costuri suplimentare, diminuarea profitului, pierderea unor clienti si oportunitati si, in unele cazuri extreme, chiar la faliment. Aceste efecte nedorite se evita prin stabilirea si aplicarea unei strategii corecte de asigurare a continuitatii activitatii si recuperare in caz de dezastru pentru sistemele informatice.



Din punct de vedere al implementarii si operarii sigure a unui sistem IT, Radu Magda (foto), General Manager la Computer Sharing Bucuresti, considera ca apar doua aspecte foarte importante si anume: “modul in care sistemul IT raspunde intr-o maniera cat mai riguroasa a tuturor cerintelor de functionalitate si, in acelasi timp, masurile ce trebuie luate pentru a se proteja infrastructura IT si informatiile stocate in cazul unor situatii neprevazute.” In general, orice organizatie, indiferent de domeniul de activitate sau marime, este pregatita pentru desfasurarea in conditii de normalitate a activitatilor esentiale pentru domeniul sau piata in care evolueaza. In aceeasi masura insa, pentru a-si asigura profitabilitatea si chiar existenta, orice organizatie trebuie sa fie pregatita si pentru operarea in conditii neobisnuite sau neasteptate. Astfel de situatii apar de regula datorita unor intreruperi neplanificate ale activitatii, crize sau dezastre. Intreruperile pot avea cauze diferite (calamitati naturale, incendii, intreruperi in furnizarea utilitatilor, atacuri informatice de diverse forme, defecte intrinseci ale elementelor de infrastructura, etc) si se pot intinde pe perioade de timp variabile (minute pana la zile si chiar saptamani sau luni).



Raspunsul industriei de IT la aceste provocari consta in dezvoltarea de solutii numite generic continuitate operationala si recuperare dupa dezastre. Iulia Tufis (foto), Project Manager la Computer Sharing Bucuresti afirma ca: “Termenul Business Continuity / Disaster Recovery (BC&DR) – Asigurarea Continuitatii Activitatilor si Recuperare in caz de Dezastru – se refera la strategii si solutii care sa permita desfasurarea sau reluarea operatiunilor in cazul unei intreruperi neasteptate sau a unui dezastru ce ar afecta buna functionare a infrastructurii ce sustine procesele critice/vitale ale unei organizatii. Planificarea BC&DR este un proces destinat

sa reduca riscul la care este expusa organizatia in cazul aparitiei unui eveniment neasteptat, care ar duce la intreruperea operatiunilor de baza pentru existenta sa. Aceasta planificare este responsabilitatea top management-ului, care trebuie sa se implice decizional in elaborarea si aplicarea planurilor BC&DR.”

Sistemele informatice au o pondere si o importanta deosebite in cadrul infrastructurii operationale, astfel ca intocmirea unui plan adecvat care asigura continuitatea sau reluarea serviciilor IT critice (IT Infrastructure Recovery Plan - IT IRP) este absolut necesara. IT IRP este parte din strategia generala pentru politica privind BC&DR adoptata de organizatie si ca atare trebuie sa fie consistent cu obiectivele ce au fost stabilite in cadrul acestei strategii. IT IRP trebuie sa fie elaborat si implementat in conformitate cu parametri de performanta adecvati pentru a asigura suportul operational corespunzator in situatii critice pentru activitatea companiei.

### **Stabilirea si punerea in practica a unei politici privind asigurarea continuitatii activitatilor si recuperarii in caz de dezastru**



Elaborarea si punerea in practica a unei solutii BC&DR este un proces care se desfasoara etapizat, conform unei metodologii menite sa asigure conceptia si implementarea unui plan adecvat, realist si util. Mihai Iacoban (foto), Certified Information System Auditor – CISA la Computer Sharing Bucuresti, prezinta pe scurt care este continutul etapelor in cadrul acestui proces:

In prima etapa – Evaluarea riscurilor (Risk assessment) - se identifica amenintarile, importanta lor si nivelul de protectie existent. Riscurile identificate si care nu au fost luate inca in considerare pot impune masuri imediate si urgente, in functie de prioritate, cost si complexitate. In aceasta etapa, ca si in celelalte etape de analiza, pentru obtinerea de informatii este utilizata tehnica chestionarelor si a interviurilor. De aceea, este necesara implicarea persoanelor cheie din majoritatea departamentelor organizatiei.

In etapa a doua se evalueaza care este impactul asupra afacerii prin expunerea la riscurile identificate anterior (Business Impact Analysis – BIA)

Aceasta activitate se desfasoara cu scopul de a determina perioada de timp in care organizatia isi permite sa nu poata executa un anumit proces de business si sa fie capabila sa isi indeplineasca totusi obiectivele.

Durata acceptabila de intrerupere pentru sistemele informatice ce sustin un proces vital, RTO (Recovery Time Objective) este un parametru esential pentru construirea solutiei de continuitate a afacerii si recuperare in caz de dezastru, timpul de recuperare al sistemelor IT trebuind sa fie mai mic sau cel mult egal decat RTO. Un alt parametru important – Recovery Point Objective (RPO) - este determinat tot in acest stadiu si se refera la completitudinea datelor care vor fi restaurate si oferite utilizatorilor finali in intervalul de timp acceptat pentru intrerupere (RTO).

In etapa a treia se analizeaza capacitatile curente de asigurare a IT BC&DR cu scopul de a determina in ce masura obiectivele stabilite in etapa BIA (RTO & RPO) sunt indeplinite de solutiile curente de recuperare in caz de dezastru implementate pentru sistemele informatice care sustin procesele critice.

In masura in care solutiile curente nu satisfac obiectivele RTO & RPO, in etapele urmatoare se proiecteaza/implementeaza o solutie care sa reduca pe cat posibil la zero diferenta intre existent si necesar.

Astfel, in aceasta etapa se identifica: datele vitale, aplicatiile critice, sistemele si legaturile de comunicatie critice, capabilitatile curente de recuperare.

In etapa a patra se stabileste o strategie privind IT BC&DR care include obligatoriu solutia de asigurare a continuitatii activitatii si de recuperare in caz de dezastru pentru infrastructura IT.

Sunt analizate cauzele diferentelor dintre obiectivele RTO & RPO si capabilitatile curente de recuperare si se identifica solutii alternative de diminuare a acestor diferente.

Aceste solutii sunt comparate din punct de vedere cost, efort, timp necesar pentru implementare, beneficii si limitari, complexitate.

La finalul acestei etape se prezinta clientului un raport sintetic privind rezultatele analizei de solutii, dar si detaliile referitoare la fiecare varianta. In baza acestui material, clientul stabileste care va fi solutia proiectata in detaliu si implementata.

Proiectarea si implementarea solutiei IT BC&DR constituie etapa a cincea care este dedicata stabilirii unui plan care sa rafineze elementele si pasii pentru punerea in practica a solutiei stabilite anterior. Se incepe cu proiectarea in detaliu a solutiei care precizeaza arhitectura exacta a solutiei: software, hardware, comunicatii, utilitati, personal implicat, spatii, cladiri, etc.

Se continua cu stabilirea planului de implementare: etape, responsabilitati, termene, criteriile de acceptanta/finalizare a etapelor si implementarea efectiva a solutiei conform planului stabilit.

In sfarsit, in etapa a sasea se elaboreaza un plan care sa controleze reactia in caz de dezastru (IT Infrastructure Recovery Plan - IT IRP), prin care solutia implementata in etapa anterioara devine cu adevarat utila. Planul cuprinde descrierea solutiei, roluri si responsabilitati ale personalului implicat, criteriile si proceduri de declarare a unei crize, proceduri tehnice de recuperare si de revenire la modul normal de operare, proceduri de intretinere/actualizare a planului, proceduri de testare periodica a planului. Acest document este un document care trebuie revizuit si verificat periodic si ori de cate ori apar modificari in infrastructura IT a organizatiei.

**Conceptul IT Governance se impune**

Radu Magda, General Manager CSB, este de parere ca “solutiile pentru IT Business Continuity & Disaster Recovery trebuie sa fie de fapt parte din strategia operationala IT a oricarei organizatii. Aceasta strategie este guvernata de politica de dezvoltare a sistemelor IT din cadrul organizatiei, care trebuie gandita si aplicata in perfecta coordonare cu misiunea si obiectivele de dezvoltare ale afacerii de baza, sau cu alte cuvinte, aplicarea conceptului de “IT Governance” – alinierea si adecvarea serviciilor IT la sistemele de control si conducere ale companiei.”

Exista multe institutii si asociatii care se ocupa cu realizarea de standarde si recomandari de buna practica prin care se indica cele mai bune metode pentru a asigura o strategie de IT Governance adecvata. Una dintre cele mai cunoscute si apreciate dintre aceste organisme este ISACA (Information Systems Audit & Control Association). Cu mai mult de 50,000 de membri in 140 de tari, ISACA este recunoscuta ca fiind liderul mondial in asigurarea IT governance, respectiv stabilirea strategiilor, managementul, controlul si securitatea sistemelor informatice. ISACA asigura si administreaza certificarile Certified Information Systems Auditor™ (CISA®) si Certified Information Security Manager™ (CISM™).

Bunele practici ale COBIT - Control Objectives for Information and related Technology, sintetizate in acest ghid si care reprezinta de fapt consensul expertilor, membri ai ISACA, ajuta la optimizarea investitiilor in IT pe de o parte si ofera elemente de referinta, de standardizare chiar, pe de alta parte. Importanta sistemelor IT in derularea oricarui tip de activitate este o certitudine, fie ca vorbim de mediul privat, de sectorul public si administratie, de utilitati, etc. Exista prevederi legale, chiar si in Romania, referitoare la evaluarea (auditarea) implementarii si/sau operarii sistemelor IT, evaluare ce trebuie efectuata de experti certificati ISACA. Aceasta abordare trebuie extinsa astfel incat sa fie controlata calitatea tuturor produselor si serviciilor IT oferite de furnizorii existenti in piata, si care sa confirme in ce masura acestea sunt aliniate conceptului de IT Governance. In acest context concret, Computer Sharing Bucuresti, prin intermediul specialistilor sai membri ISACA si certificati CISA, ofera servicii de audit si consultanta care au ca scop asistarea clientilor pentru aplicarea conceptului de IT Governance, adica integrarea si alinierea infrastructurii IT cu strategia si obiectivele globale ale organizatiei.

**Continutul acestui articol a fost realizat in urma unei mese rotunde desfasurate la sediul Computer Sharing Bucuresti (CSB), la care au participat: Radu Magda, General Manager, Iulia Tufis, Project Manager si Mihai Iacoban, Certified Information System Auditor.**